



SPYWOLF

Security Audit Report



Completed on
December 8, 2023





OVERVIEW

This audit has been prepared for **DATES** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

“

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

”





TABLE OF CONTENTS

Project Description	01
Contract Information	02
Current Stats	03
Vulnerability Check	04
Threat Levels	05
Found Threats	06-A/06-C
Good Practices	07
Tokenomics	08
Website Analysis	09
Social Media & Online Presence	10
About SPYWOLF	11
Disclaimer	12



DATES



PROJECT DESCRIPTION

According to their website:

"A cool new meme character named \$DATES is jumping into the cryptocurrency market, adding some fun to the community. Many talented developers on Binance Smart Chain (Bsc) are backing pDates, which means people who invest in \$DATES could make a lot of money."

Release Date: Launched at December 1st, 2023

Category: Meme token



CONTRACT INFO

Token Name
hsmh dates

Symbol
dates

Contract Address
0x83d93a5683F83F52D6Fd346eBBB22Aa1BE7e7f4A

Network
Binance Smart Chain

Language
Solidity

Deployment Date
Nov 25, 2023

Contract Type
Token with taxes

Total Supply
100,000

Status
Launched

TAXES

Buy Tax
5%

Sell Tax
9%

*Taxes can be changed in future



Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



TOKEN TRANSFERS STATS

Transfer Count	465
Uniq Senders	50
Uniq Receivers	103
Total Amount	454820.38145472336 dates
Median Transfer Amount	16.726553575523294 dates
Average Transfer Amount	978.1083472144588 dates
First transfer date	2023-11-25
Last transfer date	2023-12-08
Days token transferred	11

SMART CONTRACT STATS

Calls Count	661
External calls	90
Internal calls	571
Transactions count	299
Uniq Callers	54
Days contract called	8
Last transaction time	2023-12-08 15:01:18 UTC
Created	2023-12-01 22:57:48 UTC
Create TX	0x383dbab78675271c83b1e0dd2f314db3a2de0eee7f5f131b82778a5e41edf194
Creator	0x269c48c8e9e002f1357b5ae6f0fe47f46b7405dc



VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed



THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.



FOUND THREATS

⚠ Medium Risk

Owner can change contract's auto swap settings.
If swapAndLiquifyEnabled is set to true and swapThreshold is set to 0 or very low number, contract will halt, making it impossible to sell.

```
function changeSwapBackSettings(
    bool enableSwapBack,
    uint256 newSwapBackLimit
) external onlyOwner {
    swapAndLiquifyEnabled = enableSwapBack;
    swapThreshold = newSwapBackLimit;
    emit SwapBackUpdated(enableSwapBack, newSwapBackLimit);
}

function _transferFrom(
    address sender,
    address recipient,
    uint256 amount
) internal returns (bool) {
    .....
    if (
        msg.sender != pair &&
        !inSwapback &&
        swapAndLiquifyEnabled &&
        _balances[address(this)] >= swapThreshold
    ) {
        swapBack();
    }
    .....
}

function swapBack() internal lockTheSwap {
    uint256 amountToSwap = _balances[address(this)];

    address[] memory path = new address[](2);
    path[0] = address(this);
    path[1] = router.WETH();

    router.swapExactTokensForETHSupportingFeeOnTransferTokens(
        amountToSwap,
        0,
        path,
        address(this),
        block.timestamp
    );
    .....
}
```

- Recommendation:
 - Ensure that swapThreshold's value is always equal or greater than 1 token (consider decimals).



Informational

Owner can change buy/sell fees up to 9%.
Combined buy+sell = 18%.

When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make. Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```
function changeFees(  
    uint256 newRewardFee,  
    uint256 newMarketingFee,  
    uint256 extraSell  
) external onlyOwner {  
    rewardsFee = newRewardFee;  
    marketingFee = newMarketingFee;  
  
    totalFee = marketingFee.add(rewardsFee);  
    totalFeeIfSelling = totalFee + extraSell;  
    require(totalFeeIfSelling <= 9, "Fees cannot be higher than 9%");  
    emit FeesChanged(  
        newRewardFee,  
        newMarketingFee,  
        totalFee,  
        totalFeeIfSelling  
    );  
}
```



Informational

Owner can exclude address from dividends.

```
function changeIsDividendExempt(  
    address holder,  
    bool exempt  
) external onlyOwner {  
    require(holder != address(this) && holder != pair);  
    isDividendExempt[holder] = exempt;  
  
    if (exempt) {  
        dividendDistributor.setShare(holder, 0);  
    } else {  
        dividendDistributor.setShare(holder, _balances[holder]);  
    }  
    emit SetAsDividendExempt(holder, exempt);  
}
```

Owner can exclude address from fees.

When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.

```
function changeIsFeeExempt(address holder, bool exempt) external onlyOwner {  
    isFeeExempt[holder] = exempt;  
    emit SetAsFeeExempt(holder, exempt);  
}
```



RECOMMENDATIONS FOR

GOOD PRACTICES

1

Consider fundamental tradeoffs

2

Be attentive to blockchain properties

3

Ensure careful rollouts

4

Keep contracts simple

5

Stay up to date and track development

DATES

GOOD PRACTICES FOUND

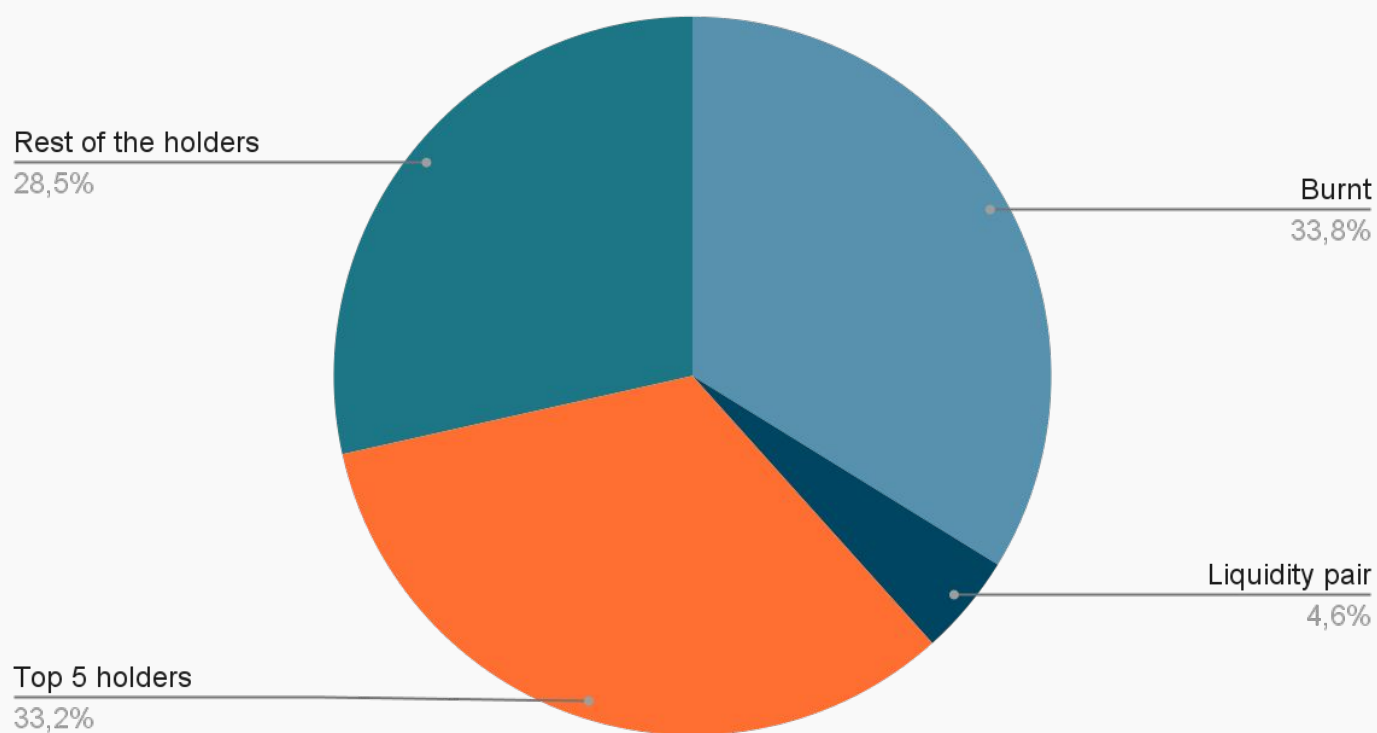
- ✓ The owner cannot mint new tokens after deployment
- ✓ The owner cannot set a transaction limit
- ✓ The smart contract utilizes "SafeMath" to prevent overflows



The following tokenomics are based on BSCScan:

- 33.8% - Burnt
- 33.15% - Top 5 holders
- 4.55% - Liquidity pair
- 28.5% - Rest of the holders

Tokens distribution



TOKENOMICS



Website URL

http://dates.lol/

Domain Registry

https://www.name.com/

Domain Expiration

2024-11-26

Technical SEO Test

Passed

Security Test

SSL certificate is not present,
proceed with caution

Design

Single page design with
appropriate color scheme
and graphics.

Content

The information helps new
investors understand what
the product does right away.
No grammar mistakes
found.

Whitepaper

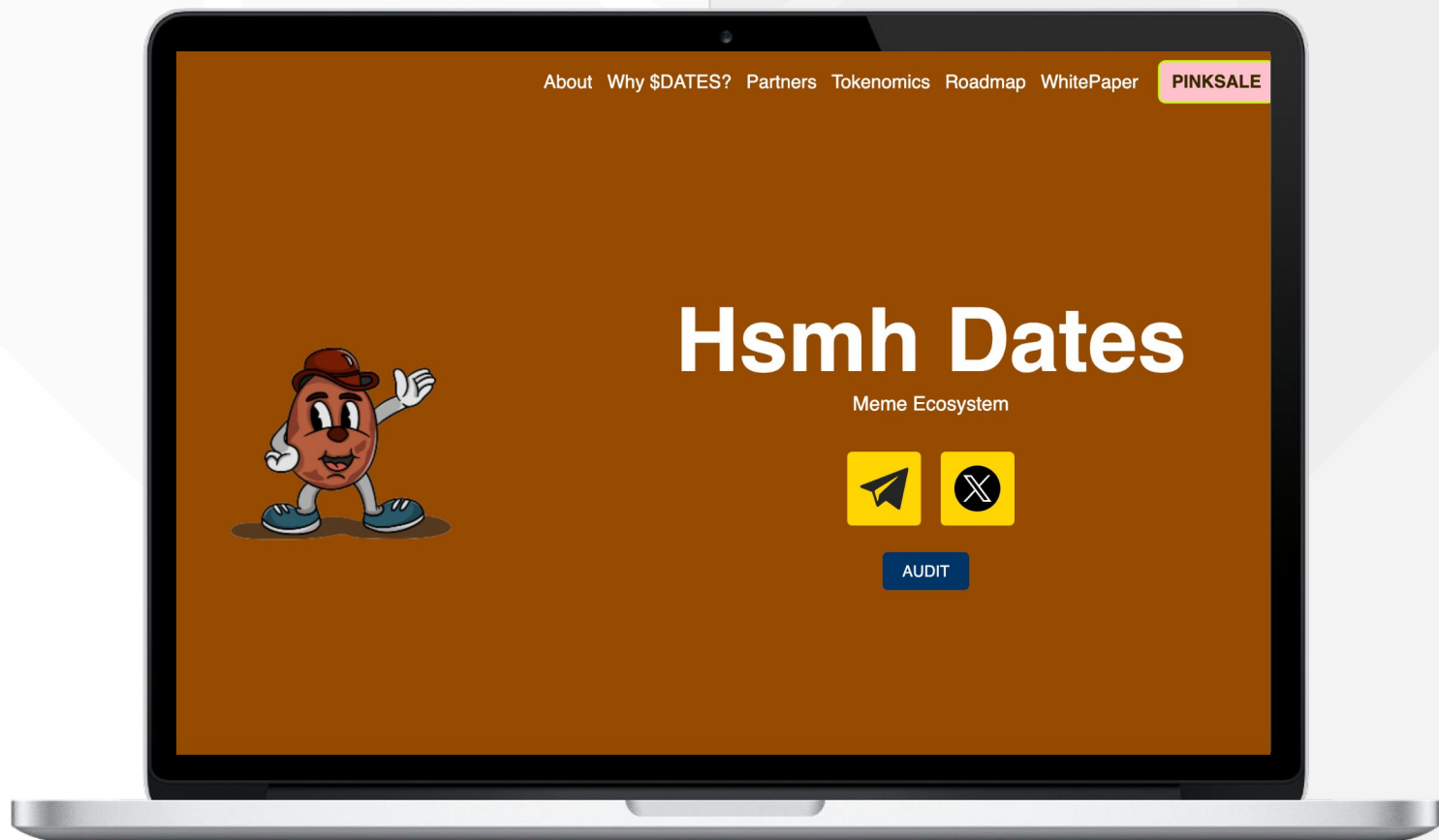
No

Roadmap

Yes, goals set without time
frames.

Mobile-friendly?

Yes



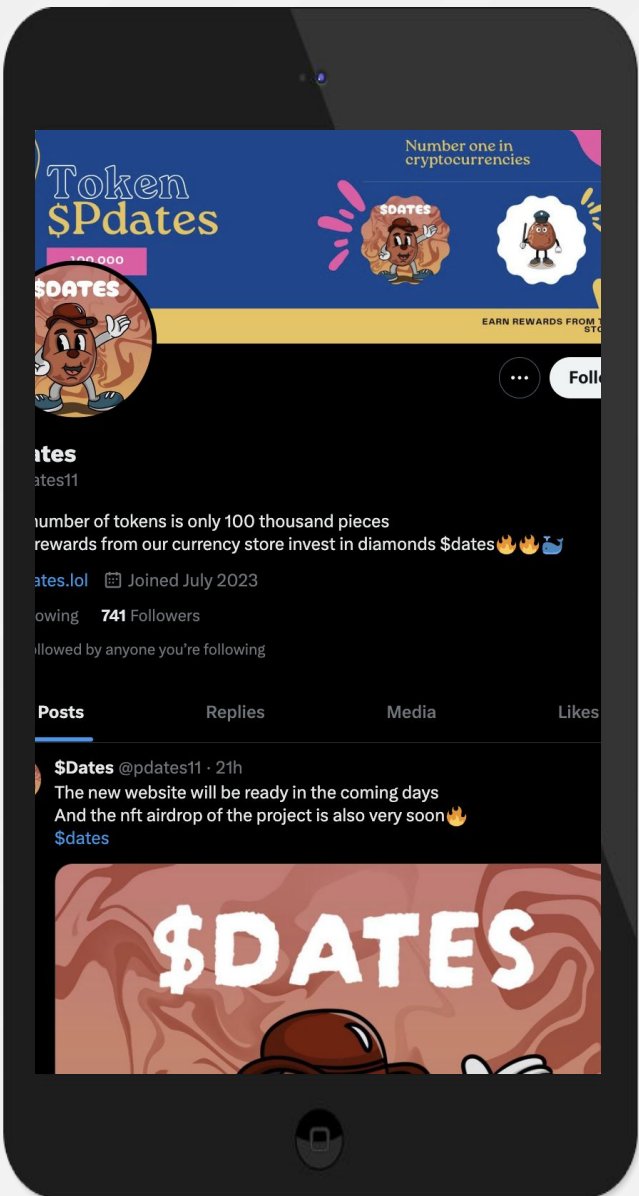
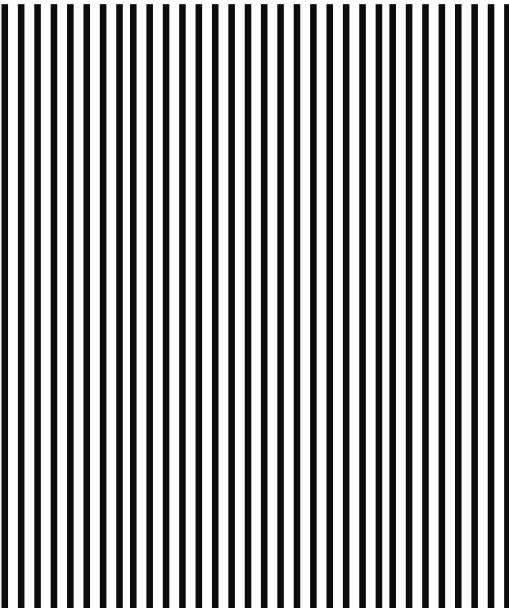
dates.lol



SOCIAL MEDIA & ONLINE PRESENCE



ANALYSIS
Project’s social media pages are active



Twitter
@pdates11

- 742 followers
- Active



Discord

- Not available



Telegram
@pdates

- 6 289 members
- Active members
- Active mods



Medium

- Not available



SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 700 SUCCESSFUL CLIENTS
- ✓ MORE THAN 1000 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE



[SPYWOLF.CO](https://spywolf.co)



[@SPYWOLFNETWORK](https://t.me/SPYWOLFNETWORK)



[@SPYWOLFNETWORK](https://twitter.com/SPYWOLFNETWORK)





Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.